transponder that provides data security for transmission between a terminal and a remote computer. The transponder provides user and terminal identification before access to a remote computer file is permitted and also provides for later secure message authentication during the course of data transmission.

In the initializing phase, a user keys in his personal identification number (PIN) to the particular computer terminal which is then sent to the encrypting transponder. Upon receipt of the PIN, the encrypting transponder generates a first key (K1) which is stored. The first key, K1, is a subset of random data stored in a fixed memory and is also a function of the PIN. The PIN is encrypted under the first key K1 and sent to the host computer which compares that number to a numbering prestored table. As such, only the encrypted PIN is sent between the encrypting transponder and the host. If the number matches the prestored value at the host computer, the host computer determines that the authorized user is at an appropriate computer terminal. As such, during the initialization operation the host computer already has a copy of an encrypted PIN number which is simply compared to a received encrypted PIN number. (See for example, column 6, lines 53-60.) The host computer then encrypts its own host identification number (HIN) and generates a first random number RN which are both encrypted under the first key K1 (see for example, columns 5-6). The host then transmits the encrypted interrogator and encrypted random number to the transponder which then are decrypted. The decrypted host identification number is compared with a prestored interrogator identification number stored in the encrypting transponder. If they match, the encrypting transponder confirms that is connected to the appropriate host computer. The system after the initialization operation is complete, then generates yet a different working key which is utilized for the remainder of the communication session and it overwrites the first key. (See for example, column 7, lines 19-35.)

As to claim 1, the office action alleges that the cited reference teaches every limitation of this claim and cites to column 5, line 57 through column 9, line 34. As best understood, it appears that the office action attempts to equate the host computer to the claimed initialization authentication unit. However, if this understanding is incorrect, Applicants respectfully request a notification of the same since the office action does not set forth any details as to which particular limitation corresponds to which structure or particular operation in the cited reference. In any event, Applicants claim a distinctly different operation. For example, Applicants claim, obtaining data representing shared data associated with the entity identification data and encrypting data based on the shared data. Also assuming for arguments sake, that the claimed shared data is equated to the first key K1 of the cited reference and that the entity identification data is equated to the personal identification number of the cited reference, Applicants claim requires that the encrypted data is communicated along with clear text entity identification data for evaluation by initialization authentication unit. As such, two pieces of information must be communicated. One is the entity identification data in a clear text fashion and the encrypted data which is encrypted based on the shared data. However, there does not appear to be a teaching or suggestion of any communication of the PIN (entity identification data) communicated in a clear text fashion along with encrypted data in the cited reference since the cited reference requires that the encrypting transponder only send the encrypted PIN that is encrypted under the first key. (See for example, column 6, lines 52-54.) As such, claim 1 is in condition for allowance. In addition, it does not appear that the host computer has any decryption capability since the host computer compares the encrypted PIN to a number in a prestored table. The host computer appears to perform some encryption, but the only decryption appears to occur in the encrypting transponder. This is also illustrated for example in the table shown in column 9, wherein the

host only performs encryption operations. As such, the host also does not compare prestored shared data to shared data derived from the encrypted data to obtain the entity identification data as required in claim 1 since no derivation appears to take place. As such, the claim is in condition for allowance.

In the alternative, if it is assumed that the encrypting transponder is the claimed initialization authentication unit, Applicants also respectfully submit that the claimed reference fails to anticipate the claimed invention. For example, the terminal 12 does not communication in a clear text fashion the PIN along with encrypted data for evaluation by the encryption transponding unit and does not appear to perform encryption during the initialization operation. In fact, it only appears that the terminal sends the personal identification number as noted in column 5, lines 57-65. Accordingly, claim 1 is believed to be in condition for allowance.

As to the dependent claims, Applicants respectfully submit that these claims add additional novel and nonobvious subject matter and Applicants respectfully reassert the relevant remarks made above with respect to claim 1. For example, claim 3 requires that the data that is encrypted includes temporal data such as date information, time of day information or other temporal information. The office action cites column 6, lines 4-10. However, Applicants respectfully submit that the cited portion only refers to the fact that the first key is a portion of a 128 bytes of random data. There is no mention of any temporal information that is encrypted. Accordingly, this claim is believed to be in condition for allowance.

Also as to claim 4 for example, the office action cites column 8, lines 39-55. However, this section refers to the interrogation code which as understood, is used for message encryption after an initialization procedure has been completed. As such, there is no method of initializing operation of an information security operation that generates second data that is a function of the

shared data and where encrypting includes encrypting the first data based on the second data. Accordingly, this claim is also believed to be in condition for allowance.

In addition, as to claim 8, this claim also includes additional novel and nonobvious subject matter in view of the cited reference. For example, the office action cites column 6, lines 4-10 and line 52 through column 7, line 17. However, the office action does not appear to identify which data within the reference corresponds to Applicants "second data as a function of the extracted prestored shared data" and as noted above, the reference does not appear to teach other limitations of claim 1. Accordingly, this claim is also believed to be in condition for allowance.

As to claim 10, for example, this claim requires that the initialization authentication unit, assumed to be the host computer decrypts the encrypted data using the second data as noted in claim 8. However, such an operation does not appear to be present in the cited reference.

As to claim 12, Applicants respectfully reassert the relevant remarks made above with respect to claim 1 and as such note that this claim is also in condition for allowance. In addition, there are other additional steps not taught or suggested by the cited reference such as, generating a copy of second data as a function of the extracted prestored shared secret data and providing a copy of the second data for use in comparing prestored shared secret data to shared secret data derived from the encrypted first data to obtain the identification data. Accordingly, this claim is also believed to be in condition for allowance.

The other dependent claims also add additional novel and nonobvious limitations and Applicants respectfully reassert the relevant remarks made above with respect to similar language in other dependent claims. Accordingly, these claims are also believed to be in condition for allowance.

As to claims 16-20, 22-23 and 25-26 since these have been rejected by a similar rationale to those of claims 1-5 and 7-11, Applicants respectfully reassert the relevant remarks with respect to claims 1-5 and 7-11 and respectfully submit that these claims are also in condition for allowance.

In addition, claims 27-31 and 33-35 have been rejected under similar rationale as to claims 1-5 and 7-9. Accordingly, Applicants respectfully reassert the relevant remarks made above with respect to claims 1-5 and 7-9 and as such Applicants respectfully submit that the claims are also in condition for allowance.

Applicants respectfully submit that the claims are now in condition for allowance and an early Notice of Allowance is earnestly solicited. The Examiner is invited to telephone the below-listed attorney if the Examiner believes that a telephone conference will expedite the prosecution of the application.

Respectfully submitted,

Date: February 4, 2004

By: _____
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P.C.
222 North LaSalle Street
Chicago, Illinois 60601
Phone: (312) 609-7599
Fax: (312) 609-5005
Email: creckamp@vedderprice.com